5. What is the impact of SSRF attacks?

SSRF attacks can have serious and wide-ranging impacts on both the **security** and **integrity** of a system. The **impact** varies depending on the attacker’s goal, the specific vulnerability exploited, and the configuration of the target system. Below are the **main impacts** of SSRF attacks:

---

1. Data Leakage

- **Description:**
  SSRF attacks can lead to the **unintended exposure** of sensitive internal data that should be protected by firewalls or other access controls.
- **Impact Examples:**
  - **Internal Databases:** The attacker may be able to access and retrieve internal database records, configuration files, or logs that are usually hidden behind internal firewalls.
  - **Cloud Metadata:** SSRF can expose **cloud instance metadata**, including sensitive data such as **credentials**, **API keys**, or **IAM roles** (e.g., AWS metadata service).
- **Real-World Example:**
  An attacker could access AWS metadata and retrieve security credentials or configuration settings that allow them to escalate their access to other systems.

---

2. Privilege Escalation

- **Description:**
  SSRF can be used to escalate privileges by accessing sensitive internal services or by exploiting misconfigurations that give attackers unauthorized access to **privileged resources**.
- **Impact Examples:**
  - **Admin Interfaces:** Accessing internal admin panels or control interfaces that are normally protected by firewalls.
  - **Internal APIs:** Gaining access to internal services (e.g., admin APIs) that are not exposed to the public internet but accessible from the server.
- **Real-World Example:**
  The attacker may be able to access a hidden admin interface at `127.0.0.1:8080` and gain administrative access to the application, escalating their privileges.

---

3. Unauthorized Access to Internal Systems

- **Description:**
  SSRF can allow attackers to interact with systems **that are not publicly exposed**. This can involve services that are **behind firewalls**, within **VPNs**, or part of **internal infrastructure**.
- **Impact Examples:**

    - **Internal Web Applications:** The attacker can query internal services that should not be exposed to the internet (e.g., databases, internal APIs).
    - **Private Networks:** SSRF can allow the attacker to probe the internal network for open ports or services (e.g., scanning internal hosts for SSH, MySQL).
- **Real-World Example:**
  An attacker can use SSRF to access private resources inside a company’s private cloud or data center that are inaccessible to external users.

---

4. Cloud Service Abuse and Data Theft

- **Description:**
  SSRF is often used to **exploit cloud environments**, especially when metadata services are involved. This could result in attackers **stealing** or **misusing cloud credentials**, leading to **further compromise**.
- **Impact Examples:**
    - **AWS Instance Metadata:** Attackers may retrieve AWS metadata to obtain instance roles and access to other cloud services (e.g., accessing an S3 bucket).
    - **Cloud Credentials:** Retrieving cloud instance API keys or IAM roles, which can then be used to **escalate** access or **pivot** to other resources.
- **Real-World Example:**
  An attacker uses SSRF to access the **AWS metadata service** and retrieves security credentials, allowing them to escalate their privileges and access sensitive resources like S3 buckets or EC2 instances.

---

5. Denial of Service (DoS)

- **Description:**
  SSRF attacks can lead to **service disruption** if the attacker causes the server to make multiple requests to an internal resource, resulting in **excessive load** and **resource exhaustion**.
- **Impact Examples:**
    - **Resource Overload:** The attacker may repeatedly request heavy or resource-consuming internal services, which may crash or overload the internal systems.
    - **Network Disruption:** Using SSRF to create network traffic that overloads internal systems or causes the system to slow down or crash.
- **Real-World Example:**
  The attacker continuously triggers SSRF requests to internal services, causing them to run out of resources or crash, leading to downtime for critical systems.

---

6. Port Scanning and Service Enumeration

- **Description:**
  Attackers can use SSRF to **scan internal networks** and identify services running on **hidden or**

protected resources. This enables further attacks on these systems.

- **Impact Examples:**
  - **Open Port Discovery:** SSRF can help attackers find open ports (e.g., port 22 for SSH, port 3306 for MySQL) on internal systems.
  - **Internal Service Mapping:** SSRF can map out internal services that were previously hidden from external attackers, revealing the architecture of internal networks.
- **Real-World Example:**
  An attacker uses SSRF to scan an internal network for open ports, identifying a vulnerable service that can be exploited in a later phase of the attack.

---

7. Remote Code Execution (RCE)

- **Description:**
  In some cases, SSRF vulnerabilities can be exploited to execute arbitrary code on internal systems or services that are exposed due to misconfigurations.
- **Impact Examples:**
  - **Command Execution:** The attacker may be able to trigger remote code execution on internal servers by making SSRF requests to vulnerable internal services or APIs.
  - **File Execution:** SSRF could cause the server to download and execute a malicious payload from an external source.
- **Real-World Example:**
  An attacker uses SSRF to make the server download and execute a malicious payload, leading to full compromise of the internal system.

---

8. Information Disclosure

- **Description:**
  SSRF can lead to the **leakage of information** about the system, such as **server configurations**, **network architecture**, and **file paths**, which can aid in further attacks.
- **Impact Examples:**
  - **Service Configuration Files:** SSRF might reveal sensitive internal files that describe how services are configured.
  - **Internal IP Addresses:** It can disclose internal IP addresses, which can be used for further attacks or to map out the infrastructure.
- **Real-World Example:**
  SSRF is used to access an internal service that reveals configuration files or internal network information, which is then used for reconnaissance.

---

9. Bypassing Authentication and Access Controls

- **Description:**
  SSRF can be used to **bypass access controls**, as the server may have greater privileges than the attacker, allowing the attacker to make requests on their behalf to **restricted resources**.
- **Impact Examples:**
  - **Bypassing VPNs or Firewalls:** The attacker might use SSRF to bypass network access controls that prevent direct access to certain resources.
  - **Accessing Admin Panels or APIs:** The attacker could force the server to access admin interfaces or internal APIs that would normally require special access credentials.
- **Real-World Example:**
  SSRF is used to bypass firewall restrictions, accessing internal resources or privileged areas of the application (e.g., internal management interfaces).

Summary of SSRF Impact

- **Data Leakage**: Exposing sensitive internal data, cloud credentials, or metadata.
- **Privilege Escalation**: Gaining higher privileges by accessing admin services.
- **Unauthorized Internal Access**: Interacting with services hidden behind firewalls.
- **Cloud Service Abuse**: Exploiting cloud metadata to steal credentials and escalate access.
- **Denial of Service (DoS)**: Overloading internal services by triggering excessive requests.
- **Port Scanning and Enumeration**: Mapping out internal services and identifying vulnerabilities.
- **Remote Code Execution**: Triggering execution of malicious code on internal servers.
- **Information Disclosure**: Revealing server configurations, network data, and file paths.
- **Bypassing Authentication**: Gaining unauthorized access to protected services.
